REMARKS

In the Official Action mailed on **13 December 2007**, Examiner reviewed claims 1-25. Claims 1-25 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Balfanz et al. ("*Talking to Strangers: Authentication in Ad-Hoc Wireless Networks*," hereinafter Balfanz) in view of Lowensohn et al. (U.S. Pub. No. 2004/0230809, hereinafter Lowensohn).

Rejection under 35 U.S.C. § 103(a)

Examiner rejected claims 1-25 under 35 U.S.C. § 103 as being unpatentable over Balfanz in view of Lowensohn. Applicant respectfully disagrees. Nothing in Balfanz or Lowensohn, either separately or in concert, discloses sending provisioning information other than information required to establish that subsequent communications are secure.

Balfanz discloses a system that follows a so-called "duckling model," wherein exchanges between two devices (called a "duckling" and a "mother") are divided into two parts. In the first part, "duckling and mother exchange secret information over a particular location-limited channel." In the second part, "the duckling uses this secret data to recognize and authenticate its mother when she contacts it over the wireless link." More specifically, Balfanz describes his system as follows:

> "Such an exchange directly captures the user's intuition that s/he wants to communicate with *that* device by using a special, *location-limited* side channel to exchange a small amount of cryptographic information. That [cryptographic] information can be used to authenticate standard key exchange protocols performed over the wireless link" (see Balfanz, section 1 (emphasis in original)).

While Balfanz discloses subsequently communicating over a wireless link using the cryptographic information, Balfanz **nowhere discloses the devices exchanging information dedicated to establishing the wireless link or providing each other with other information.**

On the other hand, Lowensohn discloses communicating user information to a "BARB base" from a "BARB badge," wherein the user information is encrypted to prevent the information from being compromised (see Lowensohn, par. [0009]-[0010] and FIG. 15B, starting with element "Approaches WS"). Because both the BARB base and the BARB badge in Lowensohn **already have the keys to enable secure communication** when they encounter one another, they begin communicating without any exchange of information to establish the wireless link. In other words, Lowensohn nowhere discloses **exchanging keys or exchanging additional information** about establishing the wireless link or providing a each other with other information.

In contrast, embodiments of the present invention provision the prospective member device with credential information and/or **other requested or default provisioning information** (see instant application, par. [0088]). For example, the prospective member device can receive provisioning information that includes "application specific information, site specific information, network specific information, or other information" (see instant application, par. [0089]). As described in the instant application:

> "This information can also include, for example but without limitation, information such as application-dependent information, device-specific assignment information (for example, in a hospital environment, the name of the patient, the case number, or other data-acquisition information required to capture data from the device or to cause the device to operate), database access information, cell phone provisioning information (such as the cell phone number), any kind of owner information, vehicle information, location information, information required to establish a secure communication link (for example … [information for establishing a

> virtual private network]), collaborative work space information, radio channel, any kind of application specific information, and information required to access a database … This additional provisioning information can contain any of the provisioning information types described above, including communication enablement information sufficient to allow the new member device to communicate on another non-preferred network connection not used during the provisioning" (see instant application, par. [0089]).

Thus, the term "provisioning" applies to the providing of a credential, as well as the providing of other information that can be used by a member device (see instant application, par. [0089]).

In summary, nothing in Balfanz or Lowensohn, separately or in concert, discloses sending provisioning information aside from the basic information required to establish that subsequent communications are secure.

Applicant has amended independent claims 1, 7, and 13 to clarify that receiving information involves receiving at least one of provisioning information or additional application-specific information, site-specific information, network-specific information, or other information that can be used by the wireless sensor from said provisioning device over said at least one preferred channel. These amendments are supported in par. [0089] of the instant application. No new matter has been added.

Applicant respectfully submits that the independent claims as presently amended are in condition for allowance. In addition, the dependent claims that depend upon these independent claims are for the same reasons in condition for allowance and for reasons of the unique combinations recited in these claims.

CONCLUSION

It is submitted that the application is presently in form for allowance. Such action is respectfully requested.

Respectfully submitted,

By /Anthony Jones/
Anthony Jones
Registration No. 59,521

Date: 13 March 2008

Anthony Jones
Park, Vaughan & Fleming LLP
2820 Fifth Street
Davis, CA 95618-7759
Tel: (530) 759-1666
Fax: (530) 759-1665
Email: tony@parklegal.com